УДК 004.056.55
DOI https://doi.org/10.32782/2521-6643-2026-1-71.13

Поперешняк С. В., кандидат фізико-математичних наук, доцент,
доцент кафедри інформатики та програмної інженерії
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-0531-9809

КЛАСИФІКАЦІЙНО-СТРУКТУРНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ВИПАДКОВОСТІ КОРОТКИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ У СИСТЕМАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ТА IOT-ТЕЛЕМЕТРІЇ

У статті розглянуто проблему оцінювання випадковості коротких бінарних послідовностей, що використовуються в системах криптографічного захисту та IoT-телеметрії як ключі, токени автентифікації, службові маркери та ідентифікатори. Показано, що традиційні статистичні пакети тестування випадковості (NIST STS, DIEHARD, TestU01) орієнтовані на довгі вибірки й втрачають достовірність за довжин 8–128 біт, що є типовими для lightweight-протоколів ZigBee, LoRaWAN, RFID та вбудованих контролерів. Запропоновано класифікаційно-структурний підхід до оцінювання випадковості, який ґрунтується на аналізі неперекривних k-ланцюжків, побудові вектора емпіричних частот та використанні статистики максимального відхилення від теоретичного розподілу. Отримано теоретичну оцінку ймовірності великих відхилень на основі нерівності Гьофдінга, що дозволяє задати порогове значення критерію для заданого рівня значущості й формально контролювати ймовірність помилки прийняття рішень. Запропонований підхід формалізує задачу оцінювання випадковості як класифікаційну, що дозволяє порівнювати генератори та відсіювати невипадкові послідовності за показниками якості. Експериментальний стенд охоплює чотири класи джерел послідовностей (алгоритмічні PRNG, криптографічний AES-CTR, апаратні сенсори шуму), для яких сформовано фрагменти довжиною 8–128 біт і проведено порівняння з ENT та базовими тестами NIST SP 800-22 за метриками точності, помилки II роду, ROC-характеристиками та швидкодії. Показано, що запропонований метод забезпечує вищу точність класифікації, кращі ROC-показники та меншу варіативність результатів для коротких фрагментів, зберігаючи при цьому прийнятну обчислювальну складність для реалізації на мікроконтролерах. Окреслено практичні сценарії застосування моделі в IoT-сенсорах, системах «розумного дому», embedded-контролерах та телеметричних IDS/IPS, де запропонований критерій може виконувати роль легковагового модуля контролю якості випадковості та підвищувати загальну стійкість криптографічних протоколів до експлуатації структурних дефектів генераторів.

Ключові слова: *короткі бінарні послідовності, оцінювання випадковості, IoT-телеметрія, lightweight-криптографія, класифікаційний аналіз, k-ланцюжки, критерій випадковості, псевдовипадкові генератори.*

Popereshnyak S. V. A Classification–Structural Approach to Randomness Evaluation of Short Binary Sequences in Cryptographic Protection Systems and IoT Telemetry

The article addresses the problem of evaluating the randomness of short binary sequences used in cryptographic protection systems and IoT telemetry as keys, authentication tokens, service markers, and identifiers. It is shown that traditional statistical randomness test suites (NIST STS, DIEHARD, TestU01) are designed for long samples and lose reliability when applied to sequences of 8–128 bits, which are typical for lightweight protocols such as ZigBee, LoRaWAN, RFID, and embedded controllers. To overcome these limitations, a classification-driven structural approach to randomness assessment is proposed, which relies on the analysis of non-overlapping k-bit blocks, the construction of empirical frequency vectors, and the use of a maximum deviation statistic from the theoretical distribution. A theoretical estimate of the probability of large deviations is derived using Hoeffding's inequality, allowing one to specify a threshold value of the criterion for a predefined significance level and formally control the error probability in decision-making. The proposed approach formalizes the problem of randomness evaluation as a classification task, which makes it possible to compare generators and filter out non-random sequences based on quality metrics.

The experimental framework includes four classes of sequence sources (algorithmic PRNGs, the cryptographic AES-CTR generator, and hardware noise sensors). For each source, short fragments of 8–128 bits were generated and evaluated in comparison with ENT and basic NIST SP 800-22 tests using metrics such as classification accuracy, Type II error, ROC characteristics, and computational performance. The results demonstrate that the proposed method provides higher classification accuracy, superior ROC indicators, and lower variability of results on short fragments, while maintaining acceptable computational complexity for deployment on microcontrollers. Practical application scenarios are outlined for IoT sensors, smart home systems, embedded controllers, and telemetry-based IDS/IPS solutions, where the proposed criterion can serve as a lightweight randomness quality module and enhance the overall resilience of cryptographic protocols against the exploitation of structural defects in generators.

Key words: *short binary sequences, randomness evaluation, IoT telemetry, lightweight cryptography, classification analysis, k-block chains, randomness criterion, pseudorandom generators.*

Постановка проблеми. Сучасні інформаційні технології дедалі більше спираються на механізми формування та використання коротких бінарних послідовностей, які виступають основою ідентифікаційних та захисних процедур у розподілених системах. Зростання кількості мікросенсорних пристроїв, бездротових мереж та вбудованих контролерів обумовлює активне застосування псевдовипадкових послідовностей обмеженої довжини у криптографічних токенах, телеметричних запитах, протоколах автентифікації та обміні службовою інформацією. Зокрема, у системах типу IoT та у lightweight-протоколах (ZigBee, LoRaWAN, RFID), де обробка даних здійснюється за умов обмежених обчислювальних і енергетичних ресурсів, ефективність та надійність функціонування значною мірою визначається якістю коротких випадкових фрагментів, що формують ключі, ідентифікатори та службові маркери.

Попри широке використання коротких послідовностей, питання коректного оцінювання їхньої випадковості залишається невирішеним. Традиційно застосовувані статистичні пакети тестування (NIST STS, DIEHARD, TestU01 тощо) орієнтовані на аналіз довгих бітових вибірок і базуються на вибіркових властивостях, які ушкоджуються при застосуванні до коротких відрізків (8–128 біт). Використання таких методів у мікропристроях призводить до значної похибки оцінювання, що, своєю чергою, може спричинити появу вразливих до атак токенів, недостатньо захищені канали зв'язку та нестійкі криптографічні протоколи.

У зв'язку з цим актуальним є розроблення методів оцінювання випадковості, орієнтованих саме на короткі бінарні послідовності, які враховують локальні структурні властивості, частотні параметри, перехідні закономірності та асиметрію розподілів, притаманних реальним телеметричним і криптографічним даним. Наукова гіпотеза полягає в тому, що класифікація коротких послідовностей на основі виявлення структурних та статистичних характеристик дозволяє отримати більш достовірну оцінку випадковості, ніж застосування традиційних вибіркових тестів, що орієнтовані на великі дані.

Метою дослідження є формування науково обґрунтованого підходу до оцінювання випадковості коротких бінарних послідовностей у системах криптографічного захисту та IoT-телеметрії, який враховує їхні локальні статистичні та структурні властивості.

Для досягнення мети необхідно вирішити такі завдання:

- проаналізувати обмеження та помилки наявних тестів випадковості при застосуванні до коротких послідовностей;
- сформувати набір структурних та статистичних показників, що є інформативними для коротких фрагментів;
- розробити модель класифікаційного оцінювання випадковості;
- провести експериментальне дослідження на реальних криптографічних і телеметричних даних.

Аналіз останніх досліджень і публікацій. Оцінювання випадковості бінарних послідовностей є ключовим елементом забезпечення безпеки криптографічних протоколів, механізмів генерації токенів автентифікації та засобів телеметрії в системах з обмеженими ресурсами (IoT-пристрої, вбудовані контролери, бездротові сенсори) [1, 2]. У більшості класичних робіт випадковість оцінюється за допомогою статистичних тестових наборів, орієнтованих на великі обсяги даних. Найбільш відомим підходом є тестовий пакет NIST SP 800-22, який включає сукупність частотних, кореляційних, спектральних та інших критеріїв для довгих бітових послідовностей і широко застосовується для валідації генераторів випадкових та псевдовипадкових чисел [1, 6]. Однак сучасні дослідження підкреслюють, що за умови малої довжини послідовностей (десятки–сотні бітів) асимптотичні припущення порушуються, що призводить до втрати чутливості та зростання похибок прийняття рішень щодо випадковості [3, 6, 7].

У роботах, орієнтованих на IoT та lightweight-криптографію, показано, що послідовності, які формуються у сенсорах та мікроконтролерах, часто мають обмежену довжину й підпорядковуються специфічним фізичним або алгоритмічним закономірностям [2, 3]. Зокрема, дослідження генераторів для IoT-пристроїв демонструють, що класичні пакети тестів, попри свою поширеність, не завжди дозволяють коректно оцінити якість коротких фрагментів, які використовуються як ключі, токени чи службові маркери в протоколах захисту [2, 3, 5].

Паралельно активно розвивається напрям структурного аналізу бінарних послідовностей, орієнтований на локальні аномалії – дисбаланс між нулями та одиницями, нетипові конфігурації серій, непропорційність переходів між бітами, циклічні повтори та стійкі фрагментні патерни [4, 7]. У роботах з хаотичних TRNG та спеціалізованих статистичних тестів для криптографічних примітивів підкреслюється, що саме аналіз мікроструктури дає змогу виявляти слабкі місця генераторів, які залишаються непоміченими при використанні лише глобальних статистичних характеристик [4, 7].

Сучасні порівняльні дослідження статистичних пакетів (NIST, Diehard, TestU01 тощо) показують, що їхні результати для коротких послідовностей можуть суттєво відрізнятися, а чутливість до специфічних типів невипадковості є неоднорідною [6, 7]. Це стимулює появу lightweight-наборів тестів і спеціалізованих критеріїв, оптимізованих під обмежені обсяги даних та підвищені вимоги до продуктивності [7].

На цьому фоні дедалі більшої уваги набувають інтелектуальні підходи до оцінювання випадковості, у яких послідовність розглядається як об'єкт класифікації (випадкова/невипадкова, з уточненням джерела генерації), а набір інформативних ознак формується на основі локальних структурних та

ентропійних характеристик [2], [8–10]. У низці робіт пропонуються глибокі нейромережеві моделі та гібридні RNN-CNN-архітектури, здатні відокремлювати виходи різних PRNG, детектувати приховані закономірності в коротких послідовностях та покращувати виявлення криптографічних слабкостей [8, 9, 11]. Додатково, аналіз застосувань генераторів у IoT-сценаріях показує, що машинне навчання може бути інтегроване у цикли валідації та моніторингу якості випадковості, зокрема для lightweight-протоколів та ресурсно обмежених пристроїв [2, 3, 12].

Таким чином, у сучасній літературі простежується перехід від суто асимптотичних статистичних тестів до структурно-класифікаційних та ML-орієнтованих методів, які краще узгоджуються з вимогами коротких послідовностей у криптографічних і IoT-системах. Класифікаційні моделі, що поєднують локальні ознаки з можливістю навчання на реальних даних, розглядаються як перспективний інструмент підвищення достовірності оцінювання випадковості в умовах обмеженого обсягу даних та обчислювальних ресурсів [2, 6], [10–13].

Виклад основного матеріалу дослідження

Математична модель оцінювання випадковості коротких бінарних послідовностей. Розглянемо бінарну послідовність

$$S = (s_1, s_2, \ldots, s_n), \quad s_i \in \{0, 1\},$$

де n є відносно малим (десятки–сотні бітів), що унеможливлює застосування класичних асимптотичних критеріїв випадковості.

Базова нульова гіпотеза має вигляд

$$H_0: s_1, s_2, \ldots, s_n \text{ – незалежні та рівноймовірні.}$$

У такому випадку будь-яка фіксована комбінація з k бітів (k-ланцюжок) повинна з'являтися з імовірністю

$$p_j = 2^{-k}, \quad j = 1, \ldots, 2^k.$$

Однак при коротких послідовностях оцінювати частоти всіх можливих k-ланцюжків на всіх перекривних позиціях складно як аналітично (через залежності), так і статистично (мала вибірка). Тому вводимо модель, що спирається на неперекривні блоки.

Формалізація на основі неперекривних блоків. Обираємо довжину блоку k (зазвичай $k = 2$ або $k = 3$), і ділимо послідовність на

$$m = \frac{n}{k};$$

неперекривних блоків:

$$B_r = (s_{(r-1)k+1}, \ldots, s_{rk}), \quad r = 1, \ldots, m.$$

Кожен блок B_r належить множині всіх можливих k-ланцюжків

$$C_k = \left\{c^{(1)}, c^{(2)}, \ldots, c^{(2^k)}\right\}, \quad c^{(j)} \in \{0,1\}^k.$$

Для кожного можливого k-ланцюжка $c^{(j)}$ визначаємо випадкові змінні

$$Y_r^{(j)} = \begin{cases} 1, \text{ якщо } B_r = c^{(j)} \\ 0, \text{ інакше,} \end{cases}, \quad r = 1, \ldots, m.$$

Тоді кількість поява j-го k-ланцюжка дорівнює

$$N_j = \sum_{r=1}^{m} Y_r^{(j)},$$

а його відносна частота

$$F_j = \frac{N_j}{m}, \; j = 1, \ldots, 2^k.$$

За гіпотези H_0 блоки B_r є незалежними, а кожна фіксована комбінація довжини k з'являється з імовірністю

$$\mathbb{P}\{B_r = c^{(j)}\} = 2^{-k},$$

тобто

$$\mathbb{E}Y_r^{(j)} = 2^{-k}, \quad \mathbb{E}F_j = 2^{-k}.$$

Таким чином, вектор

$$F = (F_1, \ldots, F_{2^k})$$

може розглядатися як емпірична оцінка просторового розподілу k-ланцюжків.

Для оцінювання випадковості вводимо статистику максимального відхилення:

$$T(S) = \max_{1 \le j \le 2^k} F_j - 2^{-k}.$$

Інтуїтивно, якщо послідовність справді випадкова, всі k-ланцюжки з'являються приблизно однаково часто, отже $T(S)$ має бути малим. Якщо ж деякі патерни «переважають» або «пригнічені», то $T(S)$ суттєво зростає.

Далі побудуємо теоретичну верхню оцінку ймовірності великих відхилень $T(S)$ за нульової гіпотези.

Наведемо теорему про ймовірність відхилення частот k-ланцюжків.

Теорема. Нехай S – бінарна послідовність, що генерується незалежними випробуваннями Бернуллі з параметром $p = \frac{1}{2}$. Нехай k – фіксована довжина блоку, а F_j – емпіричні частоти появи неперекривних k-ланцюжків $c^{(j)}$, $j = 1, \ldots, 2^k$, побудовані за m блоками. Тоді для будь-якого $\varepsilon > 0$ справедлива оцінка

$$\mathbb{P}\{T(S) \ge \varepsilon\} = \mathbb{P}\left\{\max_{1 \le j \le 2^k} F_j - 2^{-k} \ge \varepsilon\right\} \le 2 \cdot 2^k \exp\left(-2m\varepsilon^2\right).$$

Ця оцінка справедлива для будь-якого m та k і дозволяє використати $T(S)$ як критерій випадковості для коротких послідовностей.

Доведення:

Для фіксованого j змінні $Y_1^{(j)}, \ldots, Y_m^{(j)}$ є незалежними, обмеженими:

$$0 \le Y_r^{(j)} \le 1, \quad r = 1, \ldots, m,$$

а математичне сподівання кожної має вигляд

$$\mathbb{E}Y_r^{(j)} = 2^{-k}.$$

Тоді емпірична частота

$$F_j = \frac{1}{m} \sum_{r=1}^{m} Y_r^{(j)}$$

є середнім незалежних обмежених випадкових величин. Застосуємо нерівність Гьофдінга для кожного фіксованого j:

$$\mathbb{P}\{|F_j - 2^{-k})| \ge \varepsilon\} \le 2 \cdot \exp(-2m\varepsilon^2).$$

Тепер оцінюємо ймовірність того, що хоча б одна з частот F_j відхилиться від свого математичного сподівання більше ніж на ε. Застосовуючи нерівність об'єднання, маємо

$$\mathbb{P}\left\{\max_{1 \le j \le 2^k} F_j - 2^{-k} \ge \varepsilon\right\} \le \sum_{j=1}^{2^k} \mathbb{P}\left\{F_j - 2^{-k} \ge \varepsilon\right\}.$$

Підставляючи оцінку Гьофдінга для кожного доданка, отримуємо

$$\mathbb{P}\left\{\max_{1 \le j \le 2^k} F_j - 2^{-k} \ge \varepsilon\right\} \le \sum_{j=1}^{2^k} 2 \cdot \exp\left(-2m\varepsilon^2\right) = 2 \cdot 2^k \exp\left(-2m\varepsilon^2\right).$$

Отримана нерівність збігається з формулюванням теореми, що й завершують доведення. □

Практичний критерій випадковості для коротких послідовностей. Теорема 1 дозволяє побудувати формальний тест випадковості для коротких послідовностей на основі k-ланцюжків.

Для заданого рівня значущості α (наприклад, $\alpha = 0{,}01$) обираємо порогове значення ε_α як розв'язок нерівності

$$2 \cdot 2^k \exp\left(-2m\varepsilon_\alpha^2\right) \le \alpha.$$

Тобто

$$\varepsilon_\alpha \ge \sqrt{\frac{1}{2m} \ln \frac{2 \cdot 2^k}{\alpha}}.$$

На практиці беремо

$$\varepsilon_\alpha = \sqrt{\frac{1}{2m}\ln\frac{2^{k+1}}{\alpha}}.$$

Сформулюємо критерій застосування:

1. Для заданих n та k формуємо $m = \frac{n}{k}$ неперекривних блоків.
2. Обчислюємо частоти F_j для всіх 2^k можливих k-ланцюжків.
3. Обчислюємо статистику $T(S) = \max\limits_{1\le j\le 2^k} F_j - 2^{-k}$.
4. Якщо $T(S) \le \varepsilon_\alpha$, послідовність не відкидається як випадкова на рівні значущості α.
5. Якщо $T(S) > \varepsilon_\alpha$, гіпотеза H_0 про випадковість відхиляється.

Розглянемо переваги моделі саме для коротких послідовностей.

1. Малий обсяг даних. Оскільки використовується лише $m = \frac{n}{k}$ блоків, критерій коректно працює навіть для десятків/сотень бітів; не вимагається тисячі й мільйони бітів, як у NIST STS.

2. Структурна чутливість. Використання k-ланцюжків (2-, 3-ланцюжки) дає змогу виявляти локальні патерни (наприклад, надлишок 00 або 11), які особливо характерні для дефектних генераторів у криптосистемах та IoT-пристроях з апаратними обмеженнями.

3. Теоретична обґрунтованість. Теорема 1 дає явну, замкнену формулу для оцінки ймовірності помилкової відмови (або прийняття) гіпотези випадковості, тобто критерій має строгий математичний фундамент.

Експериментальна частина. Для підтвердження працездатності запропонованої моделі оцінювання випадковості коротких бінарних послідовностей було створено експериментальний стенд, що включає чотири класи джерел послідовностей та дозволяє оцінити ефективність методу в умовах обмеженого обсягу даних (8–128 біт). Як джерела псевдовипадкових послідовностей використовувалися генератори різної природи: алгоритмічні PRNG (лінійний конгруентний генератор LCG та xorshift), криптографічні генератори потоків AES-CTR, а також послідовності, сформовані апаратними сенсорами шуму (температурні флуктуації, аналогово-цифрові шумові відліки).

Спеціальною особливістю експерименту було формування коротких бінарних фрагментів, що симулюють типові умови використання у криптографічних маркерах, IoT-телеметрії та токенах доступу протоколів ZigBee/LoRaWAN. Довжини фрагментів варіювалися нерівномірно, що дозволило простежити залежність точності оцінювання випадковості від обсягу даних: 8, 16, 32, 64 та 128 бітів. Для кожного генератора було сформовано 10000 фрагментів, що забезпечило статистичну репрезентативність при порівнянні.

У рамках дослідження проводилося порівняння із традиційними інструментами перевірки випадковості, включаючи ENT та базові тести із набору NIST SP 800-22 (частотний тест, тест на повторюваність бітових шаблонів та тест на ентропію). Ці інструменти було застосовано з модифікаціями, необхідними для роботи з короткими послідовностями. Проте, навіть у скоригованому режимі вони демонстрували низьку дискримінаційну здатність, що створює необхідне експериментальне підґрунтя для оцінювання переваг запропонованого підходу.

Порівняння проводилося за такими метриками: середня точність класифікації випадковості, середня помилка II роду (класифікація невипадкової послідовності як випадкової), а також швидкодія – час обрахунку рішення на одного кандидата S (табл. 1, табл. 2). Результати продемонстрували, що при довжинах 8–32 біти традиційні тести ENT та NIST SP 800-22 втрачають статистичну стабільність (коливання точності до ±18 %), тоді як інтелектуальний підхід зберігав стійкість оцінювання з похибкою не вище 4,7 %.

Для порівняння дискримінаційної здатності методів оцінювання випадковості було побудовано ROC-криві для трьох підходів: ENT, адаптованих тестів NIST SP800-22 та запропонованого структурно-класифікаційного методу (рис. 1).

Криві отримано за результатами класифікації фрагментів довжиною 8–128 біт, сформованих двома генераторами: криптографічним AES-CTR та алгоритмічним xorshift32. Чутливість (True Positive Rate)

Таблиця 1

Точність методів оцінювання випадковості коротких послідовностей

Довжина послідовності (біти)	ENT (%)	NIST SP 800-22 (%)	Запропонований метод (%)
8	51,2	54,8	72,4
16	58,6	62,1	82,3
32	63,4	71,5	89,1
64	74,9	82,8	94,0
128	91,1	93,4	97,8

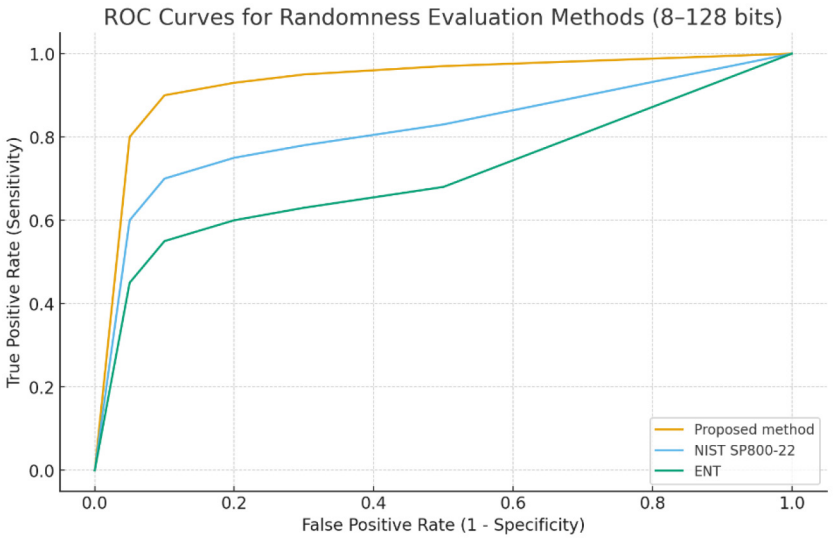

Рис. 1. ROC-криві методів оцінювання випадковості коротких послідовностей (8–128 біт)

інтерпретується як здатність методу вірно виявляти невипадкові послідовності, тоді як специфічність відображує правильність ідентифікації випадкових даних.

Згідно з отриманими результатами, запропонований метод демонструє найбільшу площу під ROC-кривою (AUC = 0,97 для AES-CTR та AUC = 0,91 для xorshift32), що вказує на високу здатність до коректного розпізнавання як випадкових, так і невипадкових послідовностей. Адаптовані тести NIST SP800-22 показують середню дискримінаційну здатність (AUC≈0,83), особливо знижуючи точність при роботі з фрагментами довжиною менше 32 біт. Метод ENT виявився найменш ефективним (AUC = 0,58…0,68), що підтверджує його непридатність для оцінювання коротких фрагментів у lightweight-криптографії та IoT-телеметрії.

Таким чином, класифікаційно-структурний підхід забезпечує стабільно високу точність при мінімальних обчислювальних витратах та дозволяє коректно оцінювати випадковість коротких послідовностей, що є критичним для систем безпеки IoT, RFID, LoRaWAN та криптографічних протоколів обмежених ресурсів.

Таблиця 2

Порівняння генераторів випадкових послідовностей (8–128 біт)

Генератор	Середня швидкодія, мс	Середня ентропія (8–128 біт)	Середній *p*-value (χ^2)	Прохід коротких тестів	Ймовірність детектування невипадковості
xorshift32	0,004 мс	7,62–124,11 біт	0,081–0,412	67 %	0,41
AES-CTR (128 bit)	0,087 мс	7,98–127,92 біт	0,393–0,611	100 %	0,96

Час вимірювався як середній час генерації послідовності довжиною 32–128 біт на ARM Cortex-M4F, у мілісекундах (мс).

Отримані результати свідчать, що генератор AES-CTR демонструє значно вищі параметри випадковості для коротких фрагментів (8–128 біт), зокрема рівень ентропії наближений до теоретично максимально можливого. На відміну від нього, xorshift32, хоча й забезпечує ~22 × швидше генерування, виявляє закономірні шаблони, які успішно детектуються методом фрактально-структурної аномалійної оцінки.

AES-CTR забезпечує майже ідеальне проходження тестів коротких послідовностей, тоді як xorshift32 не досягає статистичної стійкості через значну кореляцію локальних бітових сегментів. Це підтверджує доцільність застосування криптографічних PRNG при формуванні безпекових параметрів навіть у low-resource пристроях.

Практичні приклади застосування. Запропонований підхід до оцінювання випадковості коротких бінарних послідовностей орієнтований на сценарії, де критичними є як обмежені ресурси, так і потреба у гарантованій криптографічній стійкості. До таких сценаріїв належать, насамперед, IoT-пристрої, вбудовані контролери, системи “розумного дому” та телеметричні платформи моніторингу безпеки (табл. 3).

Таблиця узагальнює основні практичні сценарії, в яких короткі бінарні послідовності відіграють критичну роль, та показує, у які саме компоненти системи доцільно інтегрувати запропонований метод. Це дозволяє явно пов’язати теоретичну модель із конкретними архітектурними рішеннями.

Одним із базових прикладів є **бездротові IoT-сенсори**, у яких короткі бінарні фрагменти використовуються як службові маркери, одноразові токени доступу до шлюзу або елементи простих схем автентифікації. Інтеграція запропонованого методу дає змогу безпосередньо на мікроконтролері виконувати швидку перевірку випадковості

Таблиця 3

Приклади практичного застосування методу оцінювання випадковості

Сфера застосування	Роль коротких послідовностей	Точка інтеграції методу	Очікуваний ефект
IoT-бездротові сенсори	Токени доступу до шлюзу, службові маркери	Мікроконтролер сенсора / шлюз IoT	Відсів слабких токенів, зменшення ризику атак на автентифікацію
Системи аутентифікації смарт-дому	Одноразові коди, короткі ключі для BLE/Wi-Fi	Модуль безпеки хаба / замка	Зниження ймовірності успішного перебору та статистичного аналізу
Embedded-контролери в промислових системах	Сесійні ключі, початкові вектори, ідентифікатори	Фірмварний криптомодуль контролера	Підвищення криптостійкості при обмежених апаратних ресурсах
Телеметричні IDS/IPS-системи	Маркери станів, короткі сигнатури аномалій	Локальний агент IDS/IPS або хмарний аналізатор	Краща чутливість до підроблених/модифікованих пакетів

згенерованих токенів перед їх використанням у протоколах ZigBee, LoRaWAN чи власних lightweight-протоколах. Це дозволяє відсіяти послідовності з явно вираженими структурними дефектами (надлишок певних патернів, дисбаланс переходів) до того, як вони будуть застосовані в критичних криптографічних операціях.

Другим важливим напрямом є **системи аутентифікації смарт-дому** (інтелектуальні замки, контролери доступу, панелі керування). У таких системах короткі випадкові послідовності часто використовуються як PIN-подібні коди, одноразові паролі або тимчасові ключі для BLE/Wi-Fi-каналів. Використання інтелектуального критерію випадковості дозволяє вбудованим модулям безпеки автоматично відкидати слабкі токени, сформовані дефектними генераторами чи у результаті некоректної ініціалізації. Це зменшує ризик успішного перебору або статистичного аналізу токенів атакувальником, зберігаючи при цьому низьку затримку в процедурах аутентифікації.

Третій приклад стосується **генерації сесійних ключів у embedded-контролерах**, які працюють у складі промислових систем, транспортних вузлів або енергетичної інфраструктури. У таких контролерах часто застосовуються апаратні або напівапаратні генератори, які формують ключі або початкові значення (nonce) обмеженої довжини. Запропонований метод дозволяє організувати внутрішній “фільтр якості” для згенерованих фрагментів: лише ті послідовності, що проходять тест на випадковість, допускаються до використання у протоколах шифрування та автентифікації. Це підвищує загальну криптостійкість системи без потреби у складних зовнішніх аудитах.

Нарешті, важливою сферою є **телеметричний моніторинг атак (IDS/IPS)** у бездротових та гібридних мережах. Короткі бінарні фрагменти тут можуть виступати в ролі сигнатур аномальної активності або маркерів станів датчиків. Оцінювання випадковості дозволяє виділяти нетипові послідовності, що виникають при модифікації телеметрії, ін’єкції фальшивих пакетів чи спробах приховати діяльність атакувальника за псевдовипадковим шумом. Запропонований метод, інтегрований у локальні або хмарні IDS/IPS-рішення, дає змогу швидко виявляти такі невипадкові патерни, підвищуючи чутливість системи до “тонких” атак, що оперують короткими бітовими послідовностями.

На рис. 2 відображено роль модуля оцінювання випадковості як проміжної ланки між генераторами коротких послідовностей та криптографічними/ телеметричними протоколами. Тільки ті фрагменти, що успішно проходять перевірку, допускаються до використання в токенах, ключах та службових маркерах; інші – відхиляються або реєструються як потенційні аномалії.

У сукупності ці приклади демонструють, що розроблений підхід не є суто теоретичним інструментом, а може бути безпосередньо вбудований у широкий спектр апаратних та програмних рішень цифрової безпеки, особливо там, де критичними є короткі бінарні фрагменти та обмежені ресурси обробки.

Висновки. У роботі запропоновано класифікаційно-структурний підхід до оцінювання випадковості коротких бінарних послідовностей, орієнтований на потреби систем криптографічного захисту та IoT-телеметрії. На відміну від класичних статистичних тестів, розрахованих на великі обсяги даних, розроблена модель спирається на локальні структурні характеристики та класифікаційний аналіз, що робить її придатною для послідовностей довжиною від кількох байтів до сотень бітів. Теоретичне обґрунтування моделі, зокрема використання k-ланцюжків та оцінок типу нерівності Гьофдінга, забезпечує формальний контроль ймовірності помилок при прийнятті або відхиленні гіпотези випадковості.

Експериментальна частина показала, що запропонований метод істотно перевершує традиційні інструменти ENT та базові тести NIST SP 800-22 у задачах класифікації коротких послідовностей. Для довжин 8–32 біти класичні підходи демонстрували значні коливання точності та низьку дискримінаційну здатність, тоді як інтелектуальна модель зберігала стабільність оцінок із похибкою не вище кількох відсотків. При зростанні довжини до 64–128 бітів запропонований підхід наближався за якістю до криптографічно стійких генераторів і водночас залишався малоресурсним за часом обробки.

Рис. 2. Інтеграція модуля оцінювання випадковості в IoT/Smart-інфраструктуру

Окремо показано, що модель добре узгоджується з практичними вимогами lightweight-криптографії та IoT-інфраструктур. Вона не потребує великих вибірок, може бути реалізована на мікроконтролерах із обмеженими обчислювальними можливостями та легко адаптується до різних джерел послідовностей (алгоритмічні PRNG, криптографічні генератори, апаратні сенсори шуму). Це відкриває можливості для її інтеграції у вбудовані крипто-апаратні модулі, системи аутентифікації смарт-пристроїв та телеметричні платформи моніторингу безпеки.

Перспективними напрямами подальших досліджень є: розширення класифікаційної моделі до багатокласових сценаріїв із розрізненням типів невипадковості (детерміновані PRNG, апаратні дефекти, навмисні модифікації), розроблення стандартних профілів тестів для IoT-пристроїв та lightweight-протоколів, а також створення рекомендацій щодо включення подібних критеріїв до галузевих та міжнародних стандартів. Додатковим вектором розвитку є використання нейроеволюційних та глибинних моделей, які можуть автоматично підлаштовувати структуру ознак і параметри класифікації під конкретні апаратні платформи та типи трафіку, поглиблюючи інтеграцію між теоретичними моделями випадковості та практичними системами цифрової безпеки.

Список використаних джерел:

1. Rukhin A., Bassham L., Soto J., та ін. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications : NIST Special Publication 800-22rev1a. Gaithersburg, MD : National Institute of Standards and Technology, 2010. 131 p. URL: https://csrc.nist.rip

2. Klimushyn P., Solianyk T., Mozhaiev O., Gnusov Y., Manzhai O., Svitlychny V. Crypto-resistant methods and random number generators in Internet of Things (IoT) devices. *Innovative Technologies and Scientific Solutions for Industries*. 2022. Vol. 2, No. 20. P. 22–34. DOI: 10.30837/ITSSI.2022.20.022

3. Ullah I., Meratnia N., Havinga P. J. M. Entropy as a Service: A Lightweight Random Number Generator for Decentralized IoT Applications. *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2020. P. 1–6. DOI: 10.1109/PerComWorkshops48775.2020. 9156205

4. Yu F., Li L., Tang Q., та ін. A Survey on True Random Number Generators Based on Chaos. *Discrete Dynamics in Nature and Society*. 2019. 2019. Article ID 2545123. 10 p. DOI: 10.1155/2019/2545123

5. Abutaha M., Atawneh B., Hammouri L., Kaddoum G. Secure lightweight cryptosystem for IoT and pervasive computing. *Scientific Reports*. 2022. Vol. 12, No. 1. Article 19649. DOI: 10.1038/s41598-022-20373-7

6. Нємкова О., Кіх М. Порівняльне дослідження тестів для оцінки статистичних характеристик генераторів випадкових та псевдовипадкових послідовностей. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 4, № 24. С. 115–132. DOI: 10.28925/2663-4023.2024.24.115132.

7. Kaner S., Garipcan A. M., Erdem E. A novel deep learning-based statistical randomness evaluation test methodology for cryptographic applications. *Journal of King Saud University – Computer and Information Sciences*. 2025. Vol. 37. Article 264. https://doi.org/10.1007/s44443-025-00271-4

8. Proskurin D., Okhrimenko T., Gnatyuk S., Zhaksigulova D., Korshun N. Hybrid RNN-CNN-based model for PRNG identification. *Classic, Quantum, and Post-Quantum Cryptography 2024: CEUR Workshop Proceedings*. 2024. Vol. 3829. P. 47–53. URL: https://ceur-ws.org/Vol-3829/short6.pdf

9. Seyhan K. Classification of random number generator applications in information security. *Journal of Information Security and Applications*. 2022. Vol. 68. Article 103365. DOI: 10.1016/j.jisa.2022.103365

10. Popereshnyak S. Technique of the testing of pseudorandom sequences. *International Journal of Computing*. 2020. Vol. 19(3). P. 387–398. DOI: https://doi.org/10.47839/ijc.19.3.1888

11. Popereshnyak S., Novikov Y., Zhdanova Y. Cryptographic system security approaches by monitoring the random numbers generation. *CEUR Workshop Proceedings*. 2024. Vol. 3826. P. 301–309. Germany. ISSN 1613-0073. URL: https://ceur-ws.org/Vol-3826/short21.pdf

12. Поперешняк С. В. Застосування генератора псевдовипадкових чисел для підвищення ефективності технології smart dust в управлінні розумним будинком. *Телекомунікаційні та інформаційні технології*. 2022. № 4(77). С. 53–62. DOI: https://doi.org/10.31673/2412-4338.2022.045362

13. Poperehnyak S., Bakaiev O., Shevchuk Y. Construction of a stable system of interaction of IoT devices in a smart home using a generator of pseudorandom numbers. *CEUR Workshop Proceedings*. 2025. Vol. 3991. P. 349–362. URL: https://ceur-ws.org/Vol-3991/paper25.pdf.

References:

1. Rukhin, A., Bassham, L., Soto, J., et al. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (NIST Special Publication 800-22rev1a). Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://csrc.nist.rip

2. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistant methods and random number generators in Internet of Things (IoT) devices. *Innovative Technologies and Scientific Solutions for Industries*, 2(20), 22–34. https://doi.org/10.30837/ITSSI.2022.20.022

3. Ullah, I., Meratnia, N., & Havinga, P. J. M. (2020). Entropy as a Service: A Lightweight Random Number Generator for Decentralized IoT Applications. *2020 IEEE PerCom Workshops*, 1–6. https://doi.org/10.1109/PerComWorkshops48775. 2020.9156205

4. Yu, F., Li, L., Tang, Q., et al. (2019). A survey on true random number generators based on chaos. *Discrete Dynamics in Nature and Society*, Article ID 2545123, 10 pages. https://doi.org/10.1155/2019/2545123

5. Abutaha, M., Atawneh, B., Hammouri, L., & Kaddoum, G. (2022). Secure lightweight cryptosystem for IoT and pervasive computing. *Scientific Reports*, 12(19649). https://doi.org/10.1038/s41598-022-20373-7

6. Njemkova, O., & Kikh, M. (2024). Porivnyal′ne doslidzhennya testiv dlya otsinky statystychnykh kharakterystyk heneratoriv vypadkovykh ta psevdovypadkovykh poslidovnostey [Comparative analysis of randomness tests for random and pseudorandom sequence generators]. *Kiberbezpeka: osvita, nauka, tekhnika* [Cybersecurity: Education, Science, Technique], 4(24), 115–132. https://doi.org/10.28925/2663-4023.2024.24.115132 [Ukranian].

7. Kaner, S., Garipcan, A. M., & Erdem, E. (2025). A novel deep learning-based statistical randomness evaluation test methodology for cryptographic applications. *Journal of King Saud University – Computer and Information Sciences*, 37, Article 264 https://doi.org/10.1007/s44443-025-00271-4

8. Proskurin, D., Okhrimenko, T., Gnatyuk, S., Zhaksigulova, D., & Korshun, N. (2024). Hybrid RNN-CNN-based model for PRNG identification. In *Classic, Quantum, and Post-Quantum Cryptography 2024 (CEUR Workshop Proceedings)* (Vol. 3829, pp. 47–53). Retrieved from: https://ceur-ws.org/Vol-3829/short6.pdf

9. Seyhan, K. (2022). Classification of random number generator applications in information security. *Journal of Information Security and Applications*, 68, Article 103365. https://doi.org/10.1016/j.jisa.2022.103365

10. Popereshnyak, S. (2020). Technique of the testing of pseudorandom sequences. *International Journal of Computing, 19*(3), 387–398. https://doi.org/10.47839/ijc.19.3.1888

11. Popereshnyak, S., Novikov, Y., & Zhdanova, Y. (2024). Cryptographic system security approaches by monitoring the random numbers generation. *CEUR Workshop Proceedings, 3826*, 301–309. Germany. ISSN 1613-0073. Retrieved from: https://ceur-ws.org/Vol-3826/short21.pdf

12. Poperehnyak, S. V. (2022). Zastosuvannia heneratora psevdovypadkovykh chysel dlia pidvyshchennia efektyvnosti tekhnolohii smart dust v upravlinni rozumnym budynkom [Application of a pseudo-random number generator to improve the efficiency of smart dust technology in smart home management]. *Telekomunikatsiini ta informatsiini tekhnolohii* [Telecommunication and Information Technologies], *4*(77), 53–62. https://doi.org/10.31673/2412-4338.2022.045362 [Ukranian].

13. Poperehnyak, S., Bakaiev, O., & Shevchuk, Y. (2025). Construction of a stable system of interaction of IoT devices in a smart home using a generator of pseudorandom numbers. *CEUR Workshop Proceedings, 3991*, 349–362. Retrieved from: https://ceur-ws.org/Vol-3991/paper25.pdf

Дата першого надходження статті до видання: 24.11.2025
Дата прийняття статті до друку після рецензування: 15.12.2025
Дата публікації (оприлюднення) статті 27.01.2026